Universal Construction of Unitary Transformation of Quantum Computation with One- and Two-body Interactions

Xijia Miao*
Laboratory of Magnetic Resonance and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, The Chinese Academy of Sciences, Wuhan 430071, P.R.China; Department of Biochemistry, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

*correspondence address: Wuhan Institute of Physics and Mathematics. E-mail: miao@nmr.whcnc.ac.cn
April 16, 2000

Abstract

Any unitary transformation of quantum computational networks is explicitly decomposed, in an exact and unified form, into a sequence of a limited number of one-qubit quantum gates and the two-qubit diagonal gates that have diagonal unitary representation in usual computational basis. This decomposition may be simplified greatly with the help of the properties of the finite-dimensional multiple-quantum operator algebra spaces of a quantum system and the specific properties of a given quantum algorithm. As elementary building blocks of quantum computation, the two-qubit diagonal gates and one-qubit gates may be constructed physically with one- and two-body interactions in a two-state quantum system and hence could be conveniently realized experimentally. The present work will be helpful for implementing generally quantum computations with any qubits in those feasible quantum systems and determining conveniently the time evolution of these systems in course of quantum computation.

1. Introduction

Since it has been discovered that quantum computers can be much more powerful than their classical counterparts (Feynman 1982; Deutsch 1985; Shor 1994), it becomes of great practical importance to realize the quantum computers. A variety of quantum systems have been explored to build such quantum computers such as trapped ions (Cirac & Zoller 1995), nuclear spins in molecules (Gershenfeld & Chuang 1997; Cory et al. 1997) and in solid states (kane 1998), and Josephson junction arrays in superconductors (Makhlin et al. 1999), etc. Very recently, nuclear magnetic resonance

(NMR) (Ernst et al. 1987; Freeman 1997) is used to realize experimentally the Deutsch-Jozsa′s algorithm (Deutsch & Jozsa 1992, Chuang et al. 1998a) and the Grover′s algorithm (Grover 1997, Chuang et al. 1998b, Jones et al. 1998). It is expected that in the short term quantum computation with as many as ten qubits will be implemented, although there are many problems that need to be solved such as how to overcome the effects of decoherence and dephase in quantum systems and how to realize fault-tolerant and error-correlating quantum computation. Quantum computation should be performed within the characteristic time of decoherence and dephase in a quantum system. In practice, this requires that elementary building blocks of quantum computation should be chosen suitably. For example, theoretically any quantum computation should be built exactly out of a sequence of the building blocks with a length as short as possible, while these building blocks can be exactly constructed theoretically and could be physically realized conveniently in a feasible quantum system. Quantum gates were firstly suggested by Deutsch (1989) as the elementary building blocks to construct any quantum computational networks. A universal quantum gate, by copying itself and then wiring together, suffices to construct any unitary transformation of quantum computation. It has been shown theoretically (Deutsch et al. 1995, Lloyd 1995) that almost every quantum gate that operates on two or more qubits is universal, but the universal quantum gates that are really considered as conveniently realizable gates are the three-qubit gates, e.g., Toffoli′s (1981), Fredkin′s (1982), and more general Deutsch′s (1989) gate and the simpler two-qubit gates (Barenco 1995 & Sleator and Weinfurter 1995). Quantum gates with more qubits may not be universally attractive since their construction and implementation may be usually complicated in quantum systems and the theoretical construction of any unitary transformation of quantum computation out of these gates is usually not carried out easily. This may be the main reason why many investigators (DiVincenzo 1995a; Barenco 1995 & Sleator and Weinfurter 1995) have suggested the simpler universal quantum gates with only two qubits as the building blocks. Barenco et al. showed further that a set of quantum gates that consists of all one-qubit gates and the two-qubit XOR gate suffices to build any unitary transformation, although one-qubit gates and the simpler two-qubit XOR gate are not universal. However, the present theoretical composition of the three- or two-qubit universal gates or even the XOR gate along with one-qubit gates to form quantum networks usually disregards some useful properties of quantum systems and the specific properties of a given quan-

tum computation. As a consequence, it needs probably an infinite number of such quantum gates to build exactly a given unitary transformation of quantum computation. Obviously, this is impractical for quantum computation to be performed in a quantum system in which the effects of decoherence and dephase are not negligible.

In this paper any unitary transformation of quantum computational networks is decomposed explicitly as a sequence of a limited number of one- and two-body elementary propagators, i.e., one-qubit gates and the two-qubit diagonal gates $R_{kl}(\lambda_{kl}) = \exp(-i\lambda_{kl} 2 I_{kz} I_{lz})$ that have diagonal unitary representation in the conventional computational basis, in an exact and unified form. Quantum computation with any qubits is then implemented by performing the unitary transformation of a sequence of these one- and two-qubit gates on the input quantum state. In constrast to the usual composition of quantum gates to form quantum networks here is emphasized on the decomposition of a given quantum network as a sequence of the elementary building blocks. This decomposition may be simplified greatly with the aid of the properties of the finite-dimensional multiple-quantum operator algebra spaces of quantum systems (Miao, 2000a) and the specific properties of a given quantum algorithm. That the two-qubit diagonal gate $R_{kl}(\lambda_{kl})$ is chosen as an elementary building block stems from several considerations. Firstly, such choice for building blocks is beneficial to the exploitation of the properties of the finite-dimensional multiple-quantum operator algebra spaces of quantum systems to simplify the decomposition. Secondly, the two-qubit diagonal gates supplemented with all one-qubit gates suffice to construct exactly any unitary transformation of quantum computation. Thirdly, from the physically realizable point of view one-qubit gates should be the simplest gates, while according to matrix (operator) algebra properties quantum gates that have diagonal unitary representation matrices in the conventional computational bases $\{|00...00\rangle, |00...01\rangle, ..., |11...11\rangle\}$ are the elementary and simple gates. Particularly, the two-qubit diagonal gate $R_{kl}(\lambda_{kl})$ that has diagonal unitary representation matrix:

$$R_{kl}(\lambda_{kl}) = \begin{bmatrix} e^{-i\frac{1}{2}\lambda_{kl}} & & & \\ & e^{i\frac{1}{2}\lambda_{kl}} & & \\ & & e^{i\frac{1}{2}\lambda_{kl}} & \\ & & & e^{-i\frac{1}{2}\lambda_{kl}} \end{bmatrix}$$

should be the most elementary and simplest building blocks, although it is not a universal gate. Moreover, the two-qubit diagonal gate $R_{kl}(\lambda_{kl})$ can

be conveniently built up with one- and two-body interactions such as the general neighbor interaction and could be easily realized in a quantum system with N two-state particles such as coupled multispin systems in molecules or in solid states, trapped ions, superconducting Josephson junction arrays, etc. Fourthly, the two-, three-, and N-qubit (N>3) universal gates and even the XOR gate can be expressed exactly as a simple sequence of the two-qubit diagonal gates along with one-qubit gates.

2. The decomposition of unitary transformation

Quantum computation is a reversible process (Bennett, 1973). It can be thought of as a unitary transformation acted on the input state and obeys the laws of quantum mechanics (Benioff, 1980; Deutsch, 1985; DiVincenzo, 1995b). The time evolution of a quantum system from the initial state to the output state during quantum computation then can be described by a time-evolutional propagator $U(t)$ that obeys the Schrödinger equation:

$$\frac{d}{dt}U(t) = -iH(t)U(t) \qquad (\hbar = 1) \tag{1}$$

where $H(t)$ is the effective Hamiltonian for the system to perform the quantum computation. The effective Hamiltonian $H(t)$ characterizes generally the specific properties of the quantum computation. In general, quantum computational networks are composed of a sequence of quantum circuit units (Deutsch, 1989). Each such circuit unit performs the unitary transformation with a propagator $U_k(t_k)$ associated with the time-independent effective Hamiltonian H_k in the interval t_k, while the total propagator $U(t)$ can be expressed as a sequence of the propagators $U_k(t_k)$. Then it follows from Eq.(1) that

$$U(t) = \prod_k U_k(t_k) = \prod_k \exp(-iH_k t_k) \qquad (t = \sum_k t_k) \tag{2}$$

The quantum computation then can be implemented by acting a sequence of the propagators $U_k(t_k)$ on the input state. Therefore, it becomes clear that the problem to be solved is how to exactly decompose theoretically the propagators $U_k(t_k)$ of quantum circuit units as a sequence of a limited number of one- and two-qubit gates and how to build up these simple gates experimentally in an accessible quantum system. Not loss of generality, the quantum system is considered as a physical system consisting of N two-state particles. This system may be nuclear spins in molecules or in solid state, trapped ions, and superconducting Josephson junctions, etc. Here for simplification the complete decomposition of the propagators is described explicitly in a

coupled spin (I=1/2) system, which is formed by N two-state nuclei with magnetic quantum number I=1/2.

The effective Hamiltonian H_j associated with each quantum circuit unit can be generally expanded as a linear combination of base operators $\{B_k\}$ of the Liouville operator space of the spin system (Ernst, et al. 1987):

$$H_j = \sum_k a_k B_k \tag{3}$$

As suggested recently (Miao, et al. 1993 & 1997; Miao, 2000a), to determine exactly and analytically time evolution of the spin system the propagator corresponding to this Hamiltonian is first decomposed into an ordered product of a series of elementary propagators

$$U_j(t_j) = \exp(-iH_j t_j) = \prod_s R_s(\lambda_s) \tag{4}$$

The elementary propagator is defined by

$$R_s(\lambda_s) = \exp(-i\lambda_s B_s) \tag{5}$$

where λ_s is a real parameter and B_s a Hermite base operator. Obviously, the elementary propagator is also a quantum gate. Actually, the decomposition of Eq.(4) can be achieved in an exact and unified form. Firstly, the propagator $U_j(t_j)$ is converted unitarily into a diagonal unitary operator, which has diagonal unitary representation in usual computational basis, by making a sequence of elementary unitary transformations. Then each such elementary unitary transformation and the diagonal unitary operator are further decomposed into a product of a series of elementary propagators, respectively. The decomposition of Eq.(4) can be further simplified with the help of the properties of the Liouville operator spaces and its three subspaces (Miao, 2000a): the even-order multiple-quantum, the zero-quantum, and the longitudinal magnetization and spin order operator subspace. When the effective Hamiltonian H_j is a member of the longitudinal magnetization and spin order operator subspace, the propagator $U_j(t_j)$ is simply expressed as a sequence of elementary propagators built up with the base operators of the subspace (see below). If H_j is a member of the zero-quantum operator subspace, one first makes a zero-quantum unitary transformation on $U_j(t_j)$ to convert it into the diagonal unitary operator and then further decomposes the zero-quantum unitary operator and the diagonal unitary operator as a sequence of elementary propagators, respectively. When the effective Hamiltonian H_j is a member of the even-order multiple-quantum operator subspace, one makes the even-order multiple-quantum and subsequently the zero-quantum unitary transformation on $U_j(t_j)$ to convert it into the diagonal unitary operator. The even-order multiple-quantum, the zero-quantum,

and the diagonal unitary operator can be further decomposed as a sequence of elementary propagators, respectively. If H_j is not a member of any one of the above three subspaces but a member of the Liouville operator space, one first converts it unitarily into a member of the even-order multiple-quantum operator subspace by making an odd-order multiple-quantum unitary transformation on the Hamiltonian, then a further decomposition for the propagator $U_j(t_j)$ can be carried out with the help of the properties of the even-order multiple-quantum operator subspace.

It is clearly shown from the closed property of operator algebra space that any quantum gate built up with an arbitrary operator of any one of the three aforementioned operator subspaces is a non-universal gate. These gates can form another set of non-universal gates that may be different from one-qubit gates and collection of one-qubit gates and the classical gates (Deutsch, 1995).

On the basis of the decomposition of Eq.(4) time evolution of a system in the course of quantum computation can be determined directly by acting the decomposed propagator on the input state in a quantum system or on the initial density operator in a quantum ensemble with the help of the rotation transformation between any two base operators. The rotation transformation can be generally derived from the Baker-Campbell-Hausdoff formula (Ernst, et al. 1987):

$$R_s(\lambda_s)B_rR_s(\lambda_s)^{-1} = \sum_{n=0} \frac{(-i\lambda_s)^n}{n!}C_n \tag{6}$$

where $C_0 = B_r$ and $C_n = [B_s, C_{n-1}]$ and particularly, if $[B_s, [B_s, B_r]] = \alpha B_r$ the transforamtion (6) reduces to a simpler closed form

$$R_s(\lambda_s)B_rR_s(\lambda_s)^{-1} = B_r\cos(\sqrt{\alpha}\lambda_s) - \frac{i}{\sqrt{\alpha}}[B_s, B_r]\sin(\sqrt{\alpha}\lambda_s) \tag{7}$$

For a coupled N-spin (I=1/2) system the proper base operators $\{B_k\}$ of the Liouville operator space are usually chosen as the Cartesian product operators (Sϕrensen, et al. 1983; Ernst, et al. 1987):

$$\{B_k\} = \{E, I_{k_1\alpha}, 2I_{k_1\alpha}I_{k_2\beta}, ..., 2^{n-1}I_{k_1\alpha}I_{k_2\beta}...I_{k_n\delta}; 1 \le n \le N\} \tag{8}$$

where E is unit operator and $I_{k_i\alpha}$ $(\alpha, \beta, \delta = x, y, z)$ are spin angular momentum operators for the k_ith spin in the system ($I_{k_i} = \frac{1}{2}\sigma_{k_i}, \sigma$ is the Pauli$'$s operator). Such direct product operator set contains any n-body ($N \ge n \ge 1$) interaction terms $\{2^{n-1}I_{k\alpha}I_{l\beta}...I_{m\delta}\}$. It follows from Eqs.(2), (4), and (5) that the propagator $U_j(t_j)$ is usually expressed as a sequence of elementary propagators built up with any n-body ($N \ge n \ge 1$) product operators in set (8). Actually, the propagator $U_j(t_j)$ can be further expressed as a sequence of the elementary propagators built up only with one- and two-body operators

of the set (8).

Each base operator of set (8) can be converted unitarily into a member of the longitudinal magnetization and spin order operator subspace (Miao, 2000a), where the base operators of the subspace are usually chosen as the longitudinal magnetization and spin order product operators in the N-spin (I=1/2) system (Miao, et al. 1993; Miao, 2000a):

$$\{B_k^m\} = \{E, I_{kz}, 2I_{kz}I_{lz}, 4I_{kz}I_{lz}I_{mz}, ..., 2^{N-1}I_{1z}I_{2z}...I_{Nz}\} \tag{9}$$

Then any elementary propagator defined by Eq.(5) can be converted unitarily into an elementary propagator built up with a product operator of the subspace by applying a limited number of 90 degree electromagnetic pulses. A typical example is shown below

$$I_{kx}I_{ly}...I_{my}\frac{\exp(i\frac{\pi}{2}I_{ky})}{}\frac{\exp(-i\frac{\pi}{2}I_{lx})}{}.....\frac{\exp(-i\frac{\pi}{2}I_{mx})}{}\ I_{kz}I_{lz}...I_{mz}$$

where the unitary transformation $B = UAU^+$is denoted briefly as $A\overset{U}{\longrightarrow} B$. Therefore, the basic building blocks for the propagator $U_j(t_j)$ are those elementary propagators built up with the base operators of the subspace and the one-body elementary propagators of Eq.(5). On the other hand, any elementary propagator constructed with an n-body ($N \geq n \geq 1$) product operator of the subspace can be readily decomposed as a product of a series of the elementary propagators built up only with the two-body product operators in set (9) and the one-body base operators in set (8). This can be achieved by utilizing recurrently the following decomposition:

$$\exp(-i\lambda 2^n I_{k_1z}...I_{k_nz}I_{k_{n+1}z}) = V_n \exp(-i\lambda 2^{n-1} I_{k_1z}...I_{k_{n-1}z}I_{k_{n+1}z})V_n^+ \quad (n \geq 2) \tag{10}$$

where

$$V_n = \exp(-i\tfrac{\pi}{2}I_{k_{n+1}x}) \exp(-i\pi I_{k_nz}I_{k_{n+1}z}) \exp(i\tfrac{\pi}{2}I_{k_{n+1}x}) \exp(-i\tfrac{\pi}{2}I_{k_{n+1}y})$$

As a consequence, it follows from Eqs.(4) and (5) that the propagators $U_j(t_j)$ of the quantum circuit units and hence the total propagator $U(t)$ of quantum computation can be decomposed completely into a product of a series of one-body elementary propagators and the two-body diagonal elementary propagators $R_{kl}(\lambda_{kl})$ built up with the product operators $\{2I_{kz}I_{lz}\}$.

Evidently, any operator of the longitudinal magnetization and spin order operator subspace has the diagonal representation in usual computational basis and any two base operators B_r^m and B_s^m of the subspace are commutable with each other. Then any diagonal operator of the system, i.e., an operator that has diagonal representation in usual computational basis, can be expressed as a sum of the base operators of the subspace (Miao, 2000a). If

the effective Hamiltonian H_j ($=\sum_k a_k B_k^m$) associated with a quantum circuit unit is a member of the subspace, the corresponding propagator $\exp(-iH_j t_j)$ can be readily decomposed as a product of a series of elementary propagators constructed with the base operators of the subspace:

$$\exp(-iH_j t_j) = \prod_k \exp(-ia_k B_k^m t_j) \tag{11}$$

Equation (11) is very useful for the decomposition of the total propagator of a given quantum algorithm.

3. Preparation of the elementary building blocks

The two-qubit diagonal quantum gate $R_{kl}(\lambda_{kl})$ could be easily prepared in many two-state physical systems. As an example, its preparation is described explicitly in an accessible coupled N-spin (I=1/2) system. In general, the external electromagnetic field such as radiofrequency (RF) field is used to control the process of quantum computation and in the coupled spin (I=1/2) system with ravelled resonances each one-body elementary propagator defined by Eq.(5) may be prepared by utilizing selective pulses (the weak RF field) (Freeman, 1997). The spin Hamiltonian for the system in a strong static magnetic field is written as (Ernst, et al. 1987)

$$H_0 = \sum_k \Omega_k I_{kz} + \sum_{k<l} \pi J_{kl} 2I_{kz} I_{lz} \tag{12}$$

where it is assumed that the internuclear interaction is weak with respect to the Zeeman interaction and the interaction between the system and its environment, which results in decoherence and dephase, is negligible. This Hamiltonian that consists of one-body $\{I_{kz}\}$ and two-body $\{2I_{kz}I_{lz}\}$ interactions is responsible for preparing experimentally the two-qubit diagonal quantum gates $R_{kl}(\lambda_{kl})$. Figure 1 presents the quantum circuit unit (the NMR pulse sequence) for the preparation of the elementary propagator built up with the direct two-body interaction between two spins k and l, where spin echoes refocus all the undesired one- and two-body interactions and only leave selectively the desired two-body interaction $2I_{kz}I_{lz}$ in the Hamiltonian (12) by combining selective 180 degree pulses. If there is not direct interaction between any two spins k and m, their indirect two-body interaction $2I_{kz}I_{mz}$ may be achieved through a directly neighbor coupling network such as $k-l-...-s-t-m$ in the system:

$$2I_{kz}I_{mz} \underline{\exp(-i\pi I_{kx} I_{rx})}\, \underline{\exp(-i\pi I_{ky} I_{ry})}\; 2I_{rz}I_{mz} — ..... — 2I_{sz}I_{mz}$$

$$\underline{\exp(-i\pi I_{sx}I_{tx})}\,\underline{\exp(-i\pi I_{sy}I_{ty})}2I_{tz}I_{mz}$$

For quantum dots (Barenco, et al. 1995a; Loss & DiVincenzo, 1998) the diagonal gates $R_{kl}(\lambda_{kl})$ could be prepared in an analogous way to the above approach. In trapped ion system (Cirac & Zoller, 1995) the diagonal gates could be implemented by six laser pulses (see Appendix B) and in superconducting Josephson junction arrays (Makhlin, et al. 1999) they could also be prepared easily (Miao, 2000b).

4. Application to the universal quantum gates and quantum algorithms

It is easy to carry out the explicit decomposition of the total propagators for N-qubit quantum algorithms such as the Deutsch-Jozsa, Grover, quantum Fourier transform algorithm, etc. and for the two-, three-, and N-qubit (N>3) universal quantum gates. Several typical examples are given explicitly below.

4.1 The two-, three-, and any N-qubit universal quantum gates

The unitary representation matrix U_N of the N-qubit universal gate (Deutsch, 1989; Barenco, 1995 & Barenco, et al. 1995b) can be generally written as

$$U_N = E + Diag(0,0,...,0,1)\bigotimes(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}) \tag{13}$$

where the matrix $[u_{ij}]$ acting on the Nth qubit is $u(2)$ unitary matrix and can be generally expressed as

$$U(2) = T_N \exp[-i(\varphi_0 + \varphi_1 I_{Nz})]T_N^+ \tag{14}$$

where $T_N = \exp(-i\alpha I_{Nz})\exp(-i\beta I_{Ny})$. Then the unitary operation U_N can be decomposed completely as a simple sequence of one-body elementary propagators and the two-body diagonal elementary propagators:

$$U_N = T_N \exp(-i\widetilde{H}_N t)T_N^+ \qquad (t=1) \tag{15}$$

where the diagonal operator $\widetilde{H}_N$ is a member of the longitudinal magnetization and spin order operator subspace:

$$\widetilde{H}_N = \Omega_0 + \sum_{k=1}^{N} \Omega_k' I_{kz} + \sum_{l>k=1}^{N} J_{kl}' 2I_{kz}I_{lz} + \sum_{m>l>k=1}^{N} J_{klm}' 4I_{kz}I_{lz}I_{mz} + ..., \tag{16}$$

here unit operator E is omitted. All the parameters in Eqs.(14)-(16) are determined directly from the elements $\{u_{ij}\}$ of the matrix $u(2)$ (Miao, 2000a).

In particular, for the two- and three-qubit gates (Barenco, 1995 & Deutsch, 1989) the diagonal unitary operators can be respectively written as

$$\exp(-i\widetilde{H}_2 t) = \exp(-i\Omega_0)\exp(-i\Omega_1' I_{1z})\exp(-i\Omega_2' I_{2z})$$

$$\times \exp(-iJ_{12}^{'}2I_{1z}I_{2z}) \tag{17}$$

and

$$\exp(-i\widetilde{H}_3 t) = \exp(-i\Omega_0) \prod_{k=1}^{3} \exp(-i\Omega_k^{'} I_{kz}) \prod_{l>k=1}^{3} \exp(-iJ_{kl}^{'} 2I_{kz}I_{lz}) \times \exp(-iJ_{123}^{'} 4I_{1z}I_{2z}I_{3z}) \tag{18}$$

By using Eq.(10) the last three-body elementary propagator on the right-hand side of Eq.(18) can be further decomposed as a sequence of six one-body elementary propagators and three two-body diagonal elementary propagators and hence the Deutsch$^{'}$s three-qubit universal gate is exactly decomposed as a sequence of six two-qubit diagonal gates $R_{kl}(\lambda_{kl})$ and thirteen one-qubit gates and one constant phase factor.

4.2 The Grover$^{'}$s quantum search algorithm.

In most quantum algorithms the first step is the creation of a superposition. This may be achieved by applying Walsh-Hadamard transform on the groundstate in a quantum system. Any n-qubit Walsh-Hadamard transform is constructed by the direct product of n single-qubit M matrices (Grover, 1997) and can be expressed as a sequence of one-body elementary propagators and a constant phase factor:

$$W = M_1 \bigotimes M_2 \bigotimes ... \bigotimes M_n = \exp(i\tfrac{n\pi}{2}) \exp(-i\pi \sum_{k=1}^{n} I_{kx}) \exp(-i\tfrac{\pi}{2} \sum_{k=1}^{n} I_{ky})$$

In addition to the Walsh-Hadamard transform the basic unitary operations required by the Grover$^{'}$s algorithm (Grover, 1997) are the conditional phase shift operations represented respectively by the diagonal unitary matrix C and R:

$$C_{ij} = 0, \ if \ \ i \neq j; \ C_{ii} = -1; \ if \ \ i = s; \ \ C_{ii} = 1, \ if \ \ i \neq s$$

and $\quad R_{ij} = 0, \ \ if \ \ i \neq j; \ \ R_{ii} = -1, \ \ if \ \ i = 1; \ \ R_{ii} = -1, \ if \ \ i \neq 1$

The unitary operation C can be further expressed in the form of exponential operator

$$C = \exp(-iH_c t) \qquad (t = 1)$$

where the representation matrix elements of the diagonal operator H_c can be derived from the matrix C as

$$(H_c)_{ij} = 0, \ \ if \ \ i \neq j; \ \ (H_c)_{ii} = \pi, \ \ if \ \ i = s; \ \ (H_c)_{ii} = 0, \ \ if \ \ i \neq s$$

Therefore, the operator H_c is a member of the longitudinal magnetization and spin order operator subspace and can be expressed as a sum of the base operators of the subspace. It takes the same form as the diagonal operator $\widetilde{H}_N$ of Eq.(16) but with different parameters determined from the matrix

elements $\{(H_c)_{ij}\}$. As a result of Eq.(11), the unitary operation C can be decomposed into a product of elementary propagators built up with the base operators of the subspace

$$C = \exp(-i\Omega_0) \prod_{k=1} \exp(-i\Omega_k^{'} I_{kz}) \prod_{l>k=1} \exp(-iJ_{kl}^{'} 2I_{kz}I_{lz}) \times \prod_{m>l>k=1} \exp(-iJ_{klm}^{'} 4I_{kz}I_{lz}I_{mz})...$$

According to Eq.(10) the unitary operation C can be further decomposed completely as a sequence of one-body elementary propagators and the two-body diagonal elementary propagators. The diagonal phase rotation operation R can be decomposed completely in an analogous way as the unitary operation C. Thus, each of the basic unitary operations W, C, and R (the diffusion transform $D = WRW$) in any n-qubit Grover$^{'}$s algorithm is expressed explicitly as a sequence of one-qubit gates and the two-qubit diagonal gates $R_{kl}(\lambda_{kl})$. This result may be helpful to implement experimentally the algorithm with any qubits in an accessible two-state quantum system.

4.3 The Deutsch-Jozsa$^{'}$s algorithm

To decide certainly whether a function $f : B^n \longrightarrow B$ is balanced or constant, it needs to run unitary transformation U_f only once on the superposition (Deutsch & Jozsa, 1992; Jozsa, 1998; Cleve, et al. 1998):

$$U_f : \frac{1}{\sqrt{2^n}} \sum_{x_i \in B^n} |x_i\rangle [\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)] \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{x_i \in B^n} (-1)^{f(x_i)} |x_i\rangle [\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)]$$

Therefore, U_f has a diagonal unitary representation and can be expressed in the form of exponential operator:

$U_f = \exp(-iH_f t) \qquad (t = 1)$

where the diagonal operator H_f has the representation matrix elements:

$$(H_f)_{ij} = 0, \quad if \quad i \neq j; \quad (H_f)_{ij} = \begin{cases} 0, & if \quad f(x_i) = 0 \\ \pi, & if \quad f(x_i) = 1 \end{cases}$$

Obviously, any N-qubit unitary operation U_f can be readily decomposed completely in a similar way to the unitary operation C in the Grover$^{'}$s algorithm.

5. Discussion

It is widely believed that the three-qubit universal gates are sufficient to build any quantum computation (Deutsch, 1989), but several investigators (DiVincenzo, 1995a; Barenco, 1995; Sleator and Weinfurter, 1995) showed

that any three-qubit universal gates can be further expressed as a sequence of the two-qubit universal gates and hence the latters are more basic units in quantum computation. In the paper it is shown that any three- and two-qubit universal gates as well as the XOR gates can be expressed as a simple sequence of one-qubit gates and the two-qubit diagonal gates. These simple gates can be constructed with natural one- and two-body interactions such as neighbor interaction and could be readily realized experimentally in a two-state quantum system. Therefore, the two-qubit diagonal gates should be also proper elementary building blocks to construct conveniently any quantum computation physically.

The decomposition for any unitary transformation of the quantum network of a given quantum algorithm into a sequence of one-qubit gates and the two-qubit diagonal gates provides a good scheme for the quantum algorithm to be programmed on a quantum computer. The effective Hamiltonian of a given quantum algorithm characterizes generally the specific properties of the quantum algorithm and the operator algebra structure of the effective Hamiltonian may decide how the decomposition is implemented conveniently. Therefore, the decomposition may be achieved conveniently with the help of the operator algebra structure of the effective Hamiltonian and the properties of the Liouville operator space and its three operator algebra subspaces. The explicit decomposition for any unitary transformation of quantum computational networks into a sequence of one-qubit gates and the two-qubit diagonal gates in an exact and unified form will be helpful for implementing generally any N-qubit quantum computation in feasible quantum systems and determining conveniently the time evolution of these systems in course of quantum computing.

The effective Hamiltonian of a given quantum algorithm may also characterize generally the complexity of a quantum algorithm. Provided that the effective Hamiltonian consists of local interations of a quantum system subjected to the quantum algorithm, there is certainly a quantum computational network that can simulate efficiently the quantum computation (Lloyd, 1996). If a classical algorithm, which may not be efficient, is designed to solve an NP-problem in a classical digital computer and it can be translated into a quantum algorithm by replacing irreversible logic gates with the corresponding reversible gates according to the Bennett′s suggestion (Bennett, 1973), now one wants to ask: can the NP-problem be solved efficiently with the quantum algorithm on a quantum computer? Evidently, this is impossible (Deutsch, 1985 & 1989). Is there other quantum algorithm to solve efficiently

the same NP-problem? If a quantum computational network is designed according to the mathematical structure and characteristic of the NP-problem and the quantum mechanical laws and if the effective Hamiltonian of the quantum network of the quantum algorithm is local, the network can solve efficiently the NP-problem.

Acknowledgment

This work was supported by the Hong Kong University of Science and Technology and Professor Dr.T.Y.Tsong when author visited his research group in the Department of Biochemistry of the Hong Kong University of Science and Technology.

Added note: The initial version of the paper was submitted to the journal of Phys.Rev.Lett. on 2 February 1999 (Ref. number: LP7405 and the receipt date: 16 February 1999). The present paper is the modified version.

References

Barenco, A. 1995 Proc.R.Soc.Lond. A **449**, 679

Barenco, A., Deutsch, D., Ekert, A. & Jozsa, R. 1995a Phys.Rev.Lett. **74**, 4083

Barenco, A. Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P.W., Sleator, T., Smolin, J.A. & Weinfurter, H. 1995b Phys.Rev. A **52**, 3457

Bennett, C.H. 1973 IBM J.Res.Develop. **17**, 525

Benioff, P. 1980 J.Stat.Phys. **22**, 563

Chuang, I.L., Vandersypen, L.M.K., Zhou, X., Leung, D.W. & Lloyd, S. 1998a Nature **393**, 143

Chuang, I.L., Gershenfeld, N.A. & Kubinec, M. 1998b Phys.Rev.Lett. **80**, 3408

Cirac, J.I. & Zoller, P. 1995 Phys.Rev.Lett. **74**, 4091

Cory, D.G., Fahmy, A.F. & Havel, T.F. 1997 Proc.Natl.Acad.Sci. USA **94**, 1634

Cleve, R., Ekert, A., Macchiavello, C. & Mosca, M., 1998 Proc.R.Soc.Lond. A **454**, 339

Deutsch, D. 1985 Proc.R.Soc.Lond. A **400**, 97

Deutsch, D. 1989 Proc.R.Soc.Lond. A **425**, 73

Deutsch, D. & Jozsa, R. 1992 Proc.R.Soc.Lond. A **439**, 553

Deutsch, D., Barenco, A. & Ekert, A. 1995 Proc.R.Soc.Lond. A **449**, 669

DiVincenzo, D.P. 1995a Phys.Rev. A **51**, 1015
DiVincenzo, D.P. 1995b Science **270**, 255
Ernst, R.R., Bodenhausen, G. & Wokaun, A. 1987 *Principles of Nuclear Magnetic Resonance in One and Two Dimensions.* Oxford: Oxford University Press
Feynman, R.P. 1982 Int.J.Theor.Phys. **21**, 467
Fredkin, E. & Toffoli, T. 1982 Int.J.Theor.Phys. **21**, 219
Freeman, R. 1997 *Spin Choreography.* Oxford: Spektrum
Grover, L.K. 1997 Phys.Rev.Lett. **79**, 325
Gershenfeld, N.A. & Chuang, I.L. 1997 Science **275**, 350
Jones, J.A., Mosca, M. & Hansen, R.H. 1998 Nature **393**, 344
Jozsa, R. 1998 Proc.R.Soc.Lond. A **454**, 323
Kane, B.E. 1998 Nature **393**, 133
Lloyd, S. 1995 Phys.Rev.Lett. **75**, 346
Lloyd, S. 1996 Science **273**, 1073
Loss, D. & DiVincenzo, D.P. 1998 Phys.Rev. A **57**, 120
Miao, X., Han, X., & Hu, J. 1993 Sci.China A **36**, 1199
Miao, X. & Ye, C. 1997 Mol.Phys. **90**, 499
Miao, X. 2000a Molec.Phys. (in press)
Miao, X. 2000b http://xxx.lanl.gov/abs/quant-ph/0003113
Makhlin, Yu., Schön, G. & Shnirman, A. 1999 Nature **398**, 305
Sørensen, O.W., Eich, G.W., Levitt, M.H., Bodenhausen, G., & Ernst, R.R. 1983 Prog. NMR Spectrosc. **16**, 163
Shor, P.W. 1994 *Proc.35th Ann.Symp.on Found.of Computer Science*, IEEE Comp.Soc.Press, Los Alamitos, CA, pp.124
Sleator, T. & Weinfurther, H. 1995 Phys.Rev.Lett. **74**, 4087
Toffoli, T. 1981 Math.System theory **14**, 13

Appendix A
The multiple-quantum operator algebra spaces

A p-quantum operator Q_p is defined by (Miao, et al. 1993, Miao, 2000a)

$$I_z Q_p|\Psi_r\rangle = (M_r + P)Q_p|\Psi_r\rangle \qquad (\hbar = 1) \tag{A1}$$

where the wavefunction $|\Psi_r\rangle$ is an arbitrary eigenstate of the z-component I_z of the total spin angular momentum operator of a spin system with its own eigenvalue M_r

$$I_z|\Psi_r\rangle = M_r|\Psi_r\rangle \tag{A2}$$

The operator I_z is also called the total magnetic quantum operator or the total longitudinal magnetization operator of the system. The definition of

Eq.(A1) of a p-quantum operator is general and independent of energy eigenstates of the system, although the wavefunction $|\Psi_r\rangle$ is also an eigenfunction of spin Hamiltonian of the system when the contribution of Zeeman interaction to the spin Hamiltonian is dominating. However, when spin Hamiltonian of a spin system contains non-secular interactions the operator I_z usually does not commute with the spin Hamiltonian and in this case $|\Psi_r\rangle$ is not an eigenfunction of the spin Hamiltonian.

The p-quantum operator Q_p has an explicit physical meaning that a new state $Q_p|\Psi_r\rangle$ generated by Q_p acting on an arbitrary eigenstate $|\Psi_r\rangle$ is also an eigenstate of the total magnetic quantum operator I_z and its total magnetic quantum number raises p from the original one M_r. It proves easily from the definition of the p-quantum operator that the complete set of the p-quantum operators can construct a *linear subspace* of the Liouville operator space of the spin system since the sum of any two p-quantum operators is also a p-quantum operator. In particular, the complete set of zero-quantum operators is an operator algebra subspace of the Liouville operator space. This can be proven simply below. By expanding the eigenstates $|\Psi_r\rangle$ and $Q_p|\Psi_r\rangle$ in terms of the complete orthogonal and normalized eigenbase $\{|k\rangle\}$ of the operator I_z with eigenvalues $\{M_k\}$, respectively

$$|\Psi_r\rangle = \sum_k B_{rk}(0)|k\rangle, \text{ for all } k \text{ with } M_k = M_r \qquad (A3)$$

and

$$Q_p|\Psi_r\rangle = \sum_{k,l} B_{rk}(0)C_{kl}(p)|l\rangle, \qquad (A4)$$

where sums run over all indexes l with $M_l = (M_r + P)$ and k with $M_k = M_r$, respectively, one can prove easily that the product operator of any two zero-quantum operators $Q_{0\alpha}$ and $Q_{0\beta}$ is still a zero-quantum operator. It follows from Eq.(A4) that

$$Q_{0\beta}Q_{0\alpha}|\Psi_r\rangle = \sum_{k,l,m} B_{rk}(0)C^{\alpha}_{kl}(0)C^{\beta}_{lm}(0)|m\rangle \qquad (A5)$$

where sums run over all indexes k, l, m with $M_k, M_l, M_m = M_r$. Evidently, the product operator $Q_{0\beta}Q_{0\alpha}$ is still a zero-quantum operator since all the eigenstates of the operator I_z on the right-hand side of Eq.(A5) have the same eigenvalue equal to M_r of $|\Psi_r\rangle$,

$$I_z(Q_{0\beta}Q_{0\alpha})|\Psi_r\rangle = M_r(Q_{0\beta}Q_{0\alpha})|\Psi_r\rangle.$$

Therefore, all the zero-quantum operators form an operator algebra subspace of the Liouville operator space. As a direct result, the power operator $(Q_0)^n$ (n=1,2,...) of a zero-quantum operator Q_0 is a zero-quantum operator and moreover, the exponential operator $\exp(\pm i\lambda Q_0)$ of a Hermite

zero-quantum operator Q_0 is a zero-quantum unitary operator and can be expressed as a sum of base operators $\{Q_{0k}\}$ of the zero-quantum operator subspace

$$\exp(\pm i\lambda Q_0) = \sum_k \frac{(\pm i\lambda)^n}{n!}(Q_0)^n = \sum_k f_k(\pm\lambda)Q_{0k} \qquad (A6)$$

where $f_k(\pm\lambda)$ are coefficients. There is an important property of the zero-quantum operator that any p-quantum operator does not change its quantum coherence order when it is acted on by an arbitrary zero-quantum operator. The proof for the property is simple. According to the definition Eq.(A1) of a p-quantum operator and Eqs.(A2)-(A4), one has

$$Q_{0\beta}Q_pQ_{0\alpha}|\Psi_r\rangle = \sum_{k,l,m,n} B_{rk}(0)C^{\alpha}_{kl}(0)C_{lm}(p)C^{\beta}_{mn}(0)|n\rangle \qquad (A7)$$

where sums run over indexes k and l with $M_k = M_l = M_r$ as well as m and n with $M_m = M_n = (M_r + P)$, respectively. Because all the eigenstates $|n\rangle$ on the right-hand side of Eq.(A7) have the same eigenvalue $(M_r + P)$, the state $Q_{0\beta}Q_pQ_{0\alpha}|\Psi_r\rangle$ is an eigenstate of the operator I_z and its own eigenvalue equals $(M_r + P)$,

$$I_z(Q_{0\beta}Q_pQ_{0\alpha})|\Psi_r\rangle = (M_r + P)(Q_{0\beta}Q_pQ_{0\alpha})|\Psi_r\rangle \ .$$

Therefore, the product operator $Q_{0\beta}Q_pQ_{0\alpha}$ is a p-quantum operator, indicating that any p-quantum operator keeps its quantum coherence order unchanged when it is acted on by a zero-quantum operator. Particularly, any zero-quantum operator can be transferred into a sum of the base operators of the zero-quantum operator subspace by making a zero-quantum unitary transformation. This is really a direct consequence of the closed property of the zero-quantum operator subspace.

In particular, it follows from the definition of Eq.(A1) of a zero-quantum operator that all the zero-quantum operators that are commutable with each other and also commute with the total magnetic quantum operator I_z should form an operator algebra subspace of the zero-quantum operator subspace. This subspace is called the longitudinal magnetization and spin order operator subspace.

An even-order multiple-quantum operator Q_{ek} is defined by

$$Q_{ek} = \sum_p B_{kp}Q_{2p} \qquad (p = 0, \pm1, \pm2, ...) \qquad (A8)$$

where B_{kp} are coefficients and the operators Q_{2p} are $2p$-quantum operators:

$$I_zQ_{2p}|\Psi_r\rangle = (M_r + 2P)Q_{2p}|\Psi_r\rangle \qquad (A9)$$

The definition (A8) of an even-order multiple-quantum operator shows that the complete set of the even-order multiple-quantum operators is *a linear subspace* of the Liouville operator space. Here will prove further that all the

even-order multiple-quantum operators form an operator algebra subspace of the Liouville operator space. First of all, the product operator of any two $2p$-quantum operators is an even-order multiple-quantum operator. It can be found easily from Eqs.(A1)-(A4) that

$$I_z Q_{2q} Q_{2p} |\Psi_r\rangle = [M_r + 2(p+q)] Q_{2q} Q_{2p} |\Psi_r\rangle \qquad (A10)$$

This equation indicates that the product operator $Q_{2q}Q_{2p}$ is a $2(p+q)$-quantum operator, i.e., an even-order multiple-quantum operator. It turns out from Eq.(A10) and the definition Eq.(A8) of an even-order multiple-quantum operator that the product operator $Q_{ek}Q_{el}$ of any two even-order multiple-quantum operators Q_{ek} and Q_{el} is still an even-order multiple- quantum operator. Therefore, all the even-order multiple-quantum operators can form an operator algebra subspace of the Liouville operator space.

Obviously, it follows from the definition Eq.(A8) of an even-order multiple-quantum operator that the even-order multiple-quantum operator subspace contains the whole zero-quantum operator subspace.

There are some important properties of the even-order multiple-quantum operator subspace. One of which is that the exponential operator $\exp(\pm i\lambda Q_e)$ constructed with a Hermite even-order multiple-quantum operator Q_e is still an even-order multiple-quantum unitary operator and can be expressed as a sum of base operators $\{Q_{ek}\}$ of the operator subspace

$$\exp(\pm i\lambda Q_e) = \sum_p f_p(\pm\lambda) Q_{ep}. \qquad (p = 0, \pm 1, \pm 2, ...)$$

where $f_p(\pm\lambda)$ are coefficients. Another is that any even-order multiple-quantum operator is transferred into a sum of base operators of the operator subspace when it is acted on by an even-order multiple-quantum operator. These properties are obviously a direct consequence of the closed property of the even-order multiple-quantum operator algebra subspace.

The properties of the longitudinal magnetization and spin order, the zero-quantum, and the even-order multiple-quantum operator subspace of the Liouville operator space of a two-state quantum system like a spin system may be helpful for simplifying the decomposition of the time-evolutional propagator and the determination of unitary time evolution of the quantum system, and the decomposition of unitary transformations of qauntum computation into a sequence of one-qubit gates and the two-qubit diagonal quantum gates.

Appendx B

In a cold trapped ion system the two-qubit diagonal quantum gate $R_{mn}(\lambda_{mn}) = \exp(-i\lambda_{mn} 2 I_{mz} I_{nz})$ may be constructed by six laser pulses. This

elementary gate is really prepared with indirect interaction between a pair ions in the system since the interaction is set up by an intermediate media, i.e., phonon, while the direct interaction occurs between ions and phonons in the system. Adopting Cirac and Zoller′s notation (Cirac & Zoller,1995), the elementary gate for a pair of ions m and n can be explicitly prepared by the following laser pulse sequence:

$R_{mn}(\lambda_{mn}) = U_m^{1,0}(\phi_3)V_n^1(\phi_2)U_n^{1,1}(\theta_2)U_n^{1,1}(\theta_1)V_n^1(\phi_1)U_m^{1,0}(\phi_0)$

where the parameters ϕ_i $(i = 1, 2)$ and θ_i $(i = 1, 2)$ are the laser phases applied to the ion n and ϕ_i $(i = 0, 3)$ are the ones applied to the ion m, and they are not independent but subjected to the following relations:

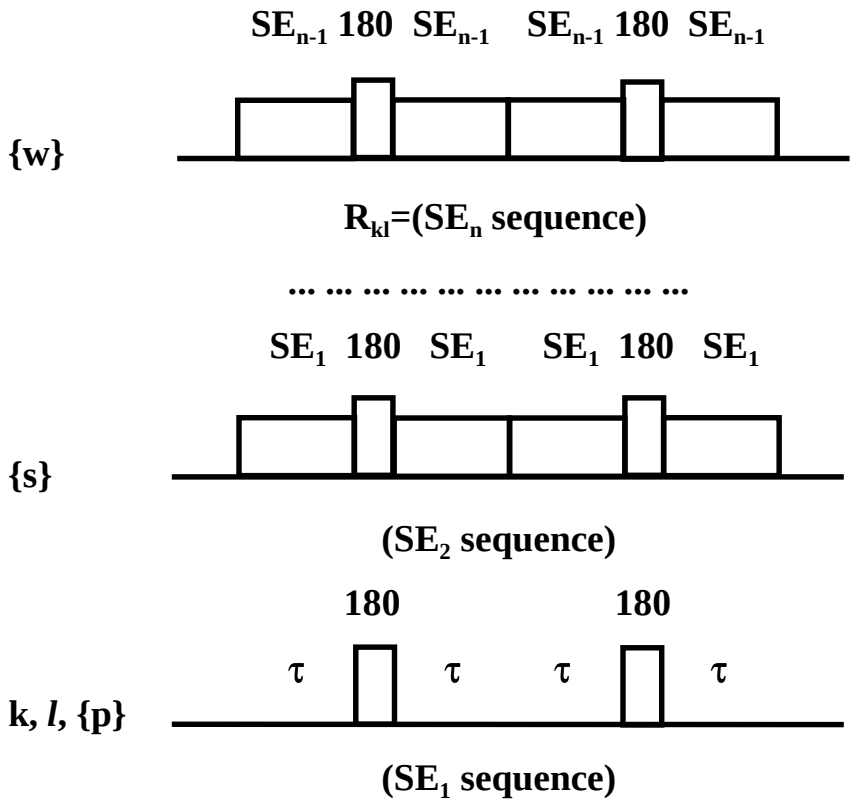
$\phi_0 - \phi_3 = \pi + 2(\phi_1 - \phi_2), \quad \theta_1 - \theta_2 = \pi + 4(\phi_1 - \phi_2).$

The parameter λ_{mn} can be determined by

$\lambda_{mn} = 2\pi - 2(\phi_1 - \phi_2)$

Therefore, by adjusting suitably the phase difference $(\phi_1 - \phi_2)$ of the lasers applied to the ion n the desired parameter λ_{mn} can be obtained.

Figure 1. The preparation for the direct two-body elementary propagator: $SE_n = R_{kl}(\lambda_{kl}) = \exp(-i\lambda_{kl}2I_{kz}I_{lz})$ $(\lambda_{kl} = 4^n\pi J_{kl}\tau)$ in a coupled N-spin (I=1/2) system with Hamiltonian of Eq.(12). The N spins except spins k and l are divided into several groups $\{p\}$, $\{s\}$, ..., $\{w\}$, where both two coupled spins k and l are not coupled with those spins of group $\{p\}$ and there may be interaction among these groups but is not coupling between any arbitrary two spins in each of these groups. The spin echo sequence SE_1 with selective 180° RF pulses applied simultaneously to the two spins k and l and all the spins of group $\{p\}$ refocuses their chemical shifts (one-body interactions) and undesired two-body interactions with any other groups but leaves the desired two-body interaction $2I_{kz}I_{lz}$. The second sequence SE_2 with four SE_1 units and selective 180° pulses applied to spins of group $\{s\}$ refocuses further one- and two-body interactions of these spins with the rest groups. Finally in sequence SE_n all the undesired one- and two-body terms are refocused but only the desired term $2I_{kz}I_{lz}$ is retained and hence $R_{kl}(\lambda_{kl})$ is obtained.


SE$_{n-1}$ 180 SE$_{n-1}$ SE$_{n-1}$ 180 SE$_{n-1}$
{w}
R$_{kl}$=(SE$_n$ sequence)
... ...
SE$_1$ 180 SE$_1$ SE$_1$ 180 SE$_1$
{s}
(SE$_2$ sequence)
180 180
τ τ τ τ
k, *l*, {p}
(SE$_1$ sequence)